Manuál k pořádání vzdělávacích simulací v oblasti digitální bezpečnosti

Úvod a účel manuálu

Manuál slouží jako doprovodný materiál k jedenácti scénářům simulací o digitální bezpečnosti. Ty lze využít v rámci školení o této oblasti. Manuál je určený pro každého, kdo chce zmíněné simulace využívat, případně vytvořit vlastní.

Na následujících řádcích proto najdete stručné vysvětlení, k čemu tyto simulace slouží a proč mohou být cennou součástí školení o digitální bezpečnosti. Podíváme se i na to, jak je naplánovat, zorganizovat i vytvořit.

Všechny obsažené scénáře byly vytvořeny ve spolupráci s novináři ze střední a východní Evropy v rámci projektu Internews Journalist Security Fellowship (JSF). Účastníci projektu je testovali na školencích, které v regionu pořádali. Tyto vzorové simulace, včetně některých verzí lokalizovaných do jazyků střední a jihovýchodní Evropy a přeložených do arabštiny a španělštiny, jsou k dispozici na tomto odkazu.

Manuál byl vytvořen především pro potřeby novinářů a redakcí v oblasti digitální bezpečnosti. Posloužit však může i pro přípravu simulací zaměřených na jiné cílové skupiny.

Co to ty simulace vůbec jsou? A v čem nám mohou pomoci?

Jde o vzdělávací metodu, která je založena na předem připraveném scénáři a interaktivní diskuzi mezi účastníky a facilitátorem. Simulační cvičení nabízí účastníkům možnost využít jejich nově nabyté zkušenosti a znalosti ve fiktivní situaci (definované scénářem), která se podobá zkušenostem z reálného života. Simulace umožňují prozkoumat širokou škálu bezpečnostních situací, jako je razie v redakci, únik dat či obtěžování v digitálním prostoru. Zatímco tradičnější metody mohou pomoci účastníkům předat jisté technické dovednosti a znalosti, simulace:

Nabízí bezpečné prostředí, kde si účastníci mohou prakticky vyzkoušet, jak se připravit a reagovat na možné bezpečnostní hrozby.

Otevírá podstatnou diskuzi o různých aspektech digitální bezpečnosti a jak se s nimi vypořádat v konkrétních kontextech a situacích. To může pomoci především účastníkům školení, kteří spolu běžně spolupracují. Mohou tak společně probrat společnou bezpečnost i bezpečnost jejich organizace.

Umožňuje zjistit, jak je jednotlivec či organizace vybavena pro řešení jednotlivých bezpečnostních výzev, se kterými se může setkat.

Simulace pomáhají jednotlivcům, organizacím i komunitám odhalit mezery ve znalostech, popsat silné stránky i limity. Pokud je simulace správně vedená, jde nad rámec poskytování informací o nástrojích a základních bezpečnostních postupech. Nemělo by chybět ani pokrytí postupů a zásad, které nemusí být nutně součástí scénáře nebo které vyžadují revizi.

Simulace jsou nejefektivnější, pokud se používají jako posilující doplněk k jiným školícím metodám. Jejich cílem totiž není primárně předat nové dovednosti a znalosti, ale spíše upevnit ty již získané pomocí scénáře, diskuze a zpětné vazby.

Z čeho se skládají scénáře simulací?
Každá z jedenácti simulací pracuje s hlavní postavou, kterou jsme pojmenovali Sára a kterou více popisujeme dále. Každý scénář obsahuje také následující součásti:

Cíl - hlavní cíl dané simulace

Vzdělávací cíle - možné vzdělávací cíle, na které se lze při procházení simulace zaměřit. Pro facilitátory je vhodnější, když se zaměří jen na některé ze vzdělávacích cílů a nesnaží se naplnit všechny.

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci - možnosti konkrétních dovedností a praktických změn chování, které si ze simulace mají účastníci odnést. Je dobré, aby si facilitátor vybral jen určité množství dovedností a přístupů chování, na které se zaměří. Ty by měly být v souladu se zvolenými vzdělávacími cíli a hlavním cílem simulace.

Scénař - scénář dané simulace. Ten obsahuje následující:

Na začátku jsou úvodní informace a kontext daného příběhu

Další informace o příběhu, které se odhalují až v průběhu simulace

Otázky a podněty pro účastníky, o kterých mohou diskutovat a na které mohou reagovat. Jsou označeny písmenem Q následovaným číslem (např. Q1, Q2, Q3 atd.).

Pod otázkami a podněty jsou uvedeny některé z potenciálních odpovědi. Ty však slouží především jako pomůcka pro facilitátora, který by je neměl účastníkům odhalit v průběhu simulace.

Některé scénáře zahrnují takzvané vstupy (budou označeny jako „vstup“). Jde o novou informaci nebo nový vývoj situace, které facilitátor může vložit do simulace, aby průběh simulace urychlich či mu dodal naopak na složitosti. Vstup může ovlivnit příběh simulace a může vyžadovat reakci či akci účastníků.

Přílohy - některé scénáře (např. Příběh 3: Obtěžování a Doxxing) obsahují i přílohy, které obvykle slouží pro potřeby zmíněných vstupů.

Vytváření scénáře pro simulaci

V rámci projektu JSF bylo vypracováno jedenáct scénářů pro simulace (ty najdete ZDE). Kdokoliv je může upravit pro potřeby svých školení a konkrétní komunity. Je možné také vytvořit úplně nové simulace. Pokud o tom přemýšlíte, případně chcete některý z již vytvořených scénářů upravit, zvažte následující:

Vzdělávací cíle by měly být jasné už na začátku tvorby daného scénáře. Měly by se vzájemně doplňovat, mít logické pořadí pro vzdělávací potřeby a být seřazeny podle důležitosti. Měly by také navazovat na hlavní cíl simulace.

Propojte vzdělávací cíle s konkrétními dovednostmi a přístupy chování, na které se mají účastníci simulace zaměřit. Usnadní to vzdělávací proces a umožní snazší měřitelnost jeho úspěšnosti. Nejlepší by bylo vzdělávací cíle přizpůsobit potřebám a zkušenostem účastníků. Je možné, že komunitu, pro kterou simulaci připravujete, již znáte, tak je vhodné to využít. V opačném případě je vhodné provést úvodní průzkum potřeb účastníků, abyste jim mohli simulaci přizpůsobit. Můžete se pobavit s částí účastníků či pro ně vytvořit krátký dotazník.

Scénář by se měl co nejvíce podobat skutečnosti. Zaměřte se na skutečné situace, výzvy a zkušenosti, ale snažte se nezmiňovat jména skutečných lidí či organizací. Ve výjimečných případech může být vhodné využít skutečná místa, v takovém případě ale zvažte možná bezpečnostní rizika a případné limity takového rozhodnutí. Práce s reálnými místy může vést například k tomu, že si o nich účastníci budou chtít zjistit co nejvíce informací, přestože to není pro simulaci podstatné a prodlužuje to její průběh.

Co se týče složitosti, scénář by neměl odvádět pozornost od vzdělávacího procesu. Umožnit účastníkům různé možnosti volby jim pomáhá pochopit, že každé jejich rozhodnutí má nějaké následky, ale zároveň ve větším počtu přidává na složitosti a prodlužuje simulaci.

V rámci scénáře můžete pracovat také s časem, různými vzpomínkami či vhledy do budoucnosti. Můžete jednotlivé události uvnitř děje ohraničit nějakým časovým obdobím, se kterým budete pracovat. Pokud se pro to rozhodnete, měli byste mít o využití těchto časových prvků jasno od začátku scénáře a udržovat přehlednost až do jeho konce.

V závislosti na úrovni dovedností facilitátora a účastníků můžete zvážit zařazení technických prvků do simulace. To by mohlo znamenat, že účastníci budou muset používat určitý nástroj, software nebo proces, aby mohli projít scénářem. Pokud se pro nějaké technické prvky rozhodnete, počítejte s časem navíc na splnění těchto úkolů a vždy mějte připravený záložní plán pro případ technických problémů. Technické prvky můžete třeba nastavit jako volitené a přizpůsobit je různým účastníkům podle jejích znalostí a zkušeností.

Můžete využít také malé či velké vstupy, které mohou či nemusí být závislé na účastnících. Obvykle jsou vstupy vhodné spíše pro delší scénáře, kdy je pro ně dostatek času. Se vstupy vždy přichází facilitátor v konkrétní čas, aby byl výsledek úspěšný, je potřeba ať má facilitátor vše připravené již

před začátkem simulací. Využití vstupů by mělo být v souladu s předem stanovenými vzdělávacími cíly.

Příprava simulace

Než se pustíte do přípravy, zamyslete se nad vaší cílovou skupinou a jak její složení může ovlivnit vzdělávací cíle. Zaměřujete se na novináře, manažery médií, lidi, kteří mají na starost bezpečnost redakcí? Každá z těchto skupin pracuje s jinými informacemi a je zodpovědná za jiná rozhodnutí. Některé simulace se záměrně mohou soustředit na širší cílovou skupinu - například na celou redakci zpravodajství, včetně vedení a bezpečnostního týmu, pro komplexní pochopení komunikace a rozhodovacích procesů. Možná také budete pracovat s účastníky, kteří mají různé úrovně dovedností, znalostí a zkušeností v oblasti digitální bezpečnosti. Věnujte proto nastavení simulace trochu více času, aby průběh co nejlépe reagoval na jejich specifické potřeby.

Pasi të keni përcaktuar audiencën tuaj të synuar, **planifikoni objektivat e të mësuarit dhe merrni parasysh aftësitë ose sjelljet specifike, për të cilat do t'i trajnoni**. Përzgjedhja e aftësive konkrete përpara trajnimit është thelbësore për t'ju ndihmuar të shtrini fokusin tuaj si trajner, të vendosni objektiva të prekshme të të mësuarit për pjesëmarrësit dhe do të ndihmojë në vendosjen e një standardi për të matur nëse trajnimi ishte efektiv. Shihni një listë të aftësive të modelit te nënseksioni brenda çdo dokumenti TTX të titulluar "Aftësi/Sjellje për t'u trajnuar para ose pas TTX". Mund të jetë tunduese të mbulohen sa më shumë objektiva të të mësuarit brenda një TTX të vetëm, por është më efektive të mbahet një trajnim më i kufizuar që mbulon objektiva të veçanta të të mësuarit. Mos harroni se audienca juaj ka një hapësirë kohe dhe vëmendje të kufizuar.

Jakmile si určíte cílovou skupinu, naplánujte si vzdělávací cíle a zvažte konkrétní dovednosti a procesy chování, na které se při školení zaměříte. Je to zásadní, abyste se mohli zaměřit na konkrétní oblast, stanovit účastníkům vhodné vzdělávací cíle a pak mohli změřit, zda jste je naplnili a školení tak bylo efektivní.

Seznam vzorových dovedností naleznete v podsekci v rámci každého scénáře s názvem „Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci“. Může se zdát vhodné pokrýt co nejvíce vzdělávacích cílů v rámci jednoho školení, efektivnější však je uspořádat simulaci zaměřenou na konkrétní vybrané cíle. Nezapomeňte, že i vaše publikum má omezený čas a pozornost.

Ujasněte si, kolik času na simulaci skutečně potřebujete. Zatímco některé vládní organizace či firmy připravují i několikadenní scénáře, je možné, že vaše cílová skupina má pro tyto aktivity mnohem méně prostoru. Berte v potaz pracovní i soukromý život účastníků. Simulace, které mají například čtyři až šest otázek nebo vstupů, běžně trvají kolem jednu až jednu a půl hodiny. Záleží samozřejmě také na velikosti skupiny. S více lidmi většinou trvá déle simulaci dokončit. Nezapomeňte si vytvořit také dostatečný prostor pro závěrečné shrnutí a diskuzi nad dosaženými vzdělávacími cíli. Proberte i to, jak účastníci získané znalosti a zkušenosti zapojí do praxe až opustí školení. Můžete tak zjistit, zda někteří nevyžadují navazující školení, ve kterém prohloubíte již získané znalosti.

Zamyslete se nad tím, kde simulaci uspořádat. Pokud se ji rozhodnete zorganizovat prezenčně, je vhodné, aby prostor umožňoval nerušenou spolupráci v průběhu simulace. Místnost se stoly a pohodlnými židlemi bude nejspíše lepší než konferenční sál. Možná budete muset zajistit také stabilní Wi-Fi připojení nebo nějakou techniku, jako je dataprojektor. Pokud je to jen trochu možné, myslete na co největší přístupnost místa (bezbariérový přístup, toalety, vhodné dopravní spojení atd.).

Rozhodněte se, zda bude stačit jeden facilitátor, nebo bude potřeba zapojit do organizace školení více lidí. Může dávat smysl, že jeden facilitátor povede simulaci, zatímco další budou pomáhat s dílčími úkoly nebo s koordinací jednotlivých skupin. Je vhodné, aby si před akcí všichni vyzkoušeli to, co mají na starosti.

Připravte si vše, co pro simulaci potřebujete. Třeba si budete potřebovat nachystat prezentaci, sehnat různé prezentační materiál, plátno nebo tabuli, na které ukážete ukážete připravené materiály, otázky, obrázky, vstuy. Nezapomeňte ani na psací potřeby či papíry, pokud je budete potřebovat.

Organizace simulací

Od tradičních školení o digitální bezpečnosti se simulace liší především v interaktivitě a praktičnosti. Při školení se očekává, že bude nejvíce mluvit školitel, který předává účastníkům své zkušenosti a znalosti. Při simulaci však sdílení zkušeností a konverzace k tématu probíhají především mezi samotnými účastníky, kteří společně přemýšlejí nad scénářem a rozhodují o příběhu.

Facilitátor v simulaci hraje zejména roli držitele procesu. Stará se o to, aby vše probíhalo hladce a účastníci splnili vytyčené cíle. Také je seznamuje se simulací, příběhem, kontextem a pozadím. Odpovídá na některé základní otázky a přidává vstupy. Zde jsou další doporučení, na co by se měl facilitátor zaměřit:

- Ujistěte se, že skutečně znáte celou simulaci.
- Nezapomeňte, jaký jste si vytyčili cíl a vzdělávací cíle. Usměrňujete diskuzi tak, aby účastníci těchto cílů dosáhli.
- Na začátku jasně seznamte účastníky s rolemi uvnitř vašeho týmu a řekněte, co se od nich očekává. V průběhu jim to připomínejte.
- Sledujte hodiny a ujistěte se, že dodržujete časový harmonogram a využíváte veškerý čas, který máte k dispozici.
- Zajistěte, že simulace probíhá v bezpečném a přívětivém prostoru, ve kterém se účastníci mohou cítit vyslyšeni a respektováni.
- Když některý účastník zmíní něco užitečného, zdůrazněte to! Může to pomoci zvýšit mezi účastníky sebevědomí a ochotu se více zapojovat.
- Když neznáte odpověď na nějakou otázku, nebojte se to přiznat a přislíbit, že odpověď zjistíte po simulaci. Využijte komunity, jako je Mattermost od Team CommUNITY, kde můžete na tyto otázky najít odpovědi.

- Pokud to jen trochu jde, zkuste sbírat zpětnou vazbu od účastníků již v průběhu simulace a to, co lze, rovnou upravte. Pokud plánujete uspořádat více simulací, zpětná vazba na konci akce vám pomůže to příště udělat lépe.
- Kdyby se náhodou simulace odklonila od původního směru, zachovejte klid. Je to v pohodě, musíte však být flexibilní a přizpůsobit změnám i závěrečné výstupy.

Chcete od nás podrobnější pokyny? Níže jsou uvedeny doporučené pokyny krok za krokem, které vám pomohou při organizaci simulace.

1. Představte se (a případné další facilitátory), vysvětlete vaše role a popište hlavní cíl simulace (například: dnes se budeme zabývat tím, jak by redakce mohla reagovat na bezpečnostní incident). To je také ideální čas, abyste si rovnou uvnitř skupiny stanovili pár základních pravidel.
2. Dále podrobněji popište, co se bude během simulace dít. Vysvětlete, že cílem je napodobit fiktivní situaci, která se blíží skutečnému životu, abychom lépe pochopili naše reakce a reakce naší komunity.
3. V závislosti na velikosti a složení skupiny můžete účastníky rozdělit do menších skupin.
4. Představte účastníkům scénář, včetně případného pozadí příběhu.
5. Scénář krok za krokem procházejte podle toho, jak se účastníkům daří zvládat jednotlivé úkoly. Buďte k dispozici pro dotazy a pomoc při řešení problémů, pokud se účastníci zaseknou.
6. Pokud je to třeba, poskytněte vstupy
7. Povzbuzujte účastníky, aby se zapojili a reagovali na podněty. Požádejte je, aby si v případě potřeby nebo užitečnosti dělali poznámky. Použijte své předem připravené odpovědi, abyste účastníkům pomohli s potížemi. Dejte jim všechny potřebné materiály, abyste se nezdržovali.
8. Poté, co účastníci simulaci dokončí, vyzvěte je k diskuzi o tom, co si z této zkušenosti odnáší. Zeptejte se je i na názory na simulační metodu jako formu školení. Je to příležitost zaznamenat zpětnou vazbu a zjistit, co příště zlepšit.
9. Po skončení simulace ověřte, zda neexistují nějaké shrnující či doplňující materiály, která by účastníci měli dostat.

Příloha 1: Základní informace o Sáře (hlavní postava simulace)

Všechny námi vytvořené scénáře pracují s hlavní postavou Sárou, která našim simulacím pomáhá dodat na jednotnosti a zároveň funguje jako dobrý výchozí bod, aby se novináři zamysleli nad konkrétními hrozbami a jejich kontextem. Sáru vám představíme níže. Tyto informace mohou facilitátoři využít, aby uvedli účastníky simulací do děje.

Sára je 41 letá novinářka. Roky pracovala pro vícero lokálních i mezinárodních médií jak v místě jejího narození, tak v sousedních zemích.

Minulý rok začala pracovat pro investigativní redakci Free Press Now, která v její zemi často přináší informace o různých politických tématech. Jde o porušování lidských práv ze strany úřadující vlády, zkorumpované vládní úředníky či o politika, který komplikuje život členům etnických menšin.

Díky svému pravdivému a spolehlivému zpravodajství se Free Press Now stal pro místní obyvatele důvěryhodným a oblíbeným zdrojem informací.

Po celostátních volbách, které se konaly před pěti měsíci, začala nová vláda u moci omezovat svobodu tisku a minulý týden úřady provedly razie v domech tří významných novinářů v hlavním městě. Nedávno byla provedena razie také v domě Sáry, přestože ti, kdo ji provedli, si odnesli pouze několik notebooků.

Příběh 1: ztracené zařízení

Vytvořeno účastníky programu JSF

Cíl

Připravit účastníky na to, jak reagovat na situaci, kdy se ztratí jedno či více jejich zařízení, které může obsahovat citlivé informace.

Vzdělávací cíle

1. Identifikovat přístupy k zajištění bezpečné komunikace mezi novináři a jejich lidskými zdroji.
2. Zlepšit povědomí o rizicích, které souvisí se ztrátou zařízení, jako je telefon nebo počítač.
3. Seznámit se s osvědčenými postupy ochrany a zabezpečení zařízení.
4. Sdílet dobrou praxi s nástupním a výstupním procesem kolegů v organizacích, především tu zaměřenou na bezpečnost zařízení.

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci

1. Instalace, nastavení a používání aplikace Signal, případně jiné aplikace pro zabezpečené zasílání zpráv
2. Nastavení a používání alternativních aplikací pro zasílání zpráv s koncovým šifrováním (například WhatsApp či tajná konverzace v aplikaci Facebook Messenger)
3. Instalace, nastavení a používání Mailvelope (či jiné šifrované e-mailové služby)
4. Šifrování mobilního zařízení (nastavení hesla)
5. Nastavení hesel pro jednotlivé aplikace v mobilním zařízení
6. Zálohování dat v mobilním zařízení a jejich šifrování (pomocí cloudových služeb nebo externího pevného disku)

Příběh

Neznámý zdroj kontaktuje Sáru přes Messenger na Facebooku. Tvrdí, že má k dispozici citlivé informace, které s ní chce sdílet. Dokument, který ji chce poskytnout, obsahuje informace o financích současného ministra obrany.

Sára chce udržet zdroj v bezpečí, a proto ho chce přesvědčit, aby informace předával přes aplikaci, která je zabezpečena koncovým šifrováním.

Otázka (O) 1: Jak může Sára svému zdroji vysvětlit princip fungování koncového šifrování, aby ho přesvědčila o důležitosti tohoto nástroje?

- Nikdo - ani společnost, která službu provozuje - nebude mít přístup k obsahu zprávy. Obsah zprávy nebude uložen v nezašifrované podobě ani na serverech společnosti
- Bezpečnostní složky nemohou soubor od poskytovatele komunikační platformy získat
- Pokud se útočníkovi podaří dostat do účtu, který byl použit k odeslání zprávy, nebude mít přístup k obsahu zpráv (pokud však neexistují nešifrované zálohy)

O2: Jaké formy digitální komunikace by měla Sara s tímto zdrojem zvážit, aby zajistila bezpečnost společné budoucí komunikace?

- Komunikační aplikace s koncovým šifrováním a mizejícími zprávami
- Šifrovaný e-mail

Zdroj je spokojený s tím, že Sáře záleží na tom, aby jejich komunikace byla bezpečná. Přesto si však stále není jistý, na jakou metodu se zaměřit. Proto ji žádá o radu s chatovacími aplikacemi, jako je Signal, Telegram, Facebook Messenger, ale také jeho e-mail.

O3 (Možnosti na výběr) - z pohledu digitální bezpečnosti: jaké jsou hlavní faktory ke zvážení při výběru a používání různých chatovacích aplikací?

- Telefonní čísla: většina komunikačních aplikací, které jsou opatřeny koncovým šifrováním, vyžadují zadání telefonního čísla. Jelikož v řadě zemí musí být čísla registrovaná na konkrétního člověka, vláda může zjistit, kdo se za daným číslem skrývá. To znamená, že v případě, kdy vláda bude mít přístup do telefonu od Sary či jejího zdroje, bude schopna určit, že spolu tito dva lidé komunikují, a to i v případě, že budou používat přezdívky či mizející zprávy (jediným zmírněním by bylo vymazání jmen z kontaktů, messengerů a v ideálním případě dát telefon do továrního nastavení)
- Tajné konverzace: Aplikace jako Facebook Messenger nebo Telegram nabízejí dva komunikační režimy, kdy jeden je opatřen koncovým šifrováním. Tento režim se běžně označuje jako „tajná konverzace“ či podobným slovním spojením. Často je potřeba tento režim zprovoznit v nastavení dané aplikace
- Mizející zprávy: v podstatě každá současná aplikace pro zasílání zpráv nabízí možnost takzvaných mizejících zpráv. Někdy je však tato funkce dostupná pouze v režimu tajné konverzace
- Smazání konverzace: jde sice o snadný krok, je ale důležité si uvědomit, že některé aplikace “smazané” konverzace pouze archivují a neodstraňují je kompletně
- Opatrnost při práci se snímky obrazovky: kterýkoli účastník konverzace se zlými úmysly může jednoduše pořídit snímek obrazovky. A pokud to aplikace neumožňuje, jednoduše si obrazovku může vyfotit pomocí jiného zařízení
- Dvoufázové ověření: útočník se může zmocnit účtu v aplikaci pro zasílání zpráv, když má přístup k zařízení s registrovaným telefonním číslem. Stačí na něj odeslat ověřovací SMS, přihlásit se na jiném zařízení a může se vydávat za vlastníka účtu. U

řady aplikací však nedostane přístup k historii konverzací a většina z nich také nyní umožňuje vyžadovat k přístupu vedle SMS kódu také další heslo. Takže i kdyby se útočníkovi podařilo zneužít telefonní číslo, bez daného hesla by pro něj bylo těžší se do účtu nabourat
- Silná hesla nebo přístupové fráze pro přihlášení k samotnému zařízení (telefonu)

O4 (možnosti na výběr) - Které jsou z pohledu digitální bezpečnosti hlavní faktory, pokud komunikujeme e-mailem?

- Zdroj by si měl vytvořit novou e-mailovou adresu čistě pro komunikaci se Sárou
- Nový e-mail by měl být zabezpečen silným a unikátním heslem a vhodným dvoufázovým ověřením
- Zdroj by si měl dát pozor na phishingové útoky a používat nástroje, které by mohly zmírnit jejich dopad. Může jít o fyzické bezpečnostní klíče nebo o správce hesel, které automaticky vyplní přístupové údaje u stránek, kde si je uložil
- V ideálním případě by měl zdroj se Sárou komunikovat přes PGP, například s využitím služby Mailvelope. Tak zajistí, že i v případě, kdy útočník získá přístup k jejich účtům, nebude schopen přečíst obsah konverzací bez jejich PGP klíče.

Zdroj poslal Sáře soubor, který si Sára prohlédla na telefonu. Je za informaci ráda a jde to s kamarády oslavit. Během párty telefon ztratí a následně si uvědomí, že na něm má velmi jednoduché heslo (1111).

O5 - Co se může stát se Sářiným telefonem a informacemi v něm?

- Kdokoli telefon najde se může dostat k citlivým informacím v případě, že se mu je podaří najít
- Nálezce by se mohl vydávat za Sáru a oslovit její kontakty
- Kdokoli se dostane k informacím v telefonu je schopen ohrozit identitu i bezpečnost Sářiných kontaktů, stejně tak shromáždit informace pro účely manipulativního sociálního inženýrství
- Sára může ztratit svou novinářskou kredibilitu

O6 - Co může Sára udělat, aby omezila dopad na svou digitální bezpečnost?

- Pokud to nastavení zařízení umožňuje, může ho na dálku smazat
- Může se přes jiné zařízení přihlásit do svého e-mailu či do účtů na sociálních sítích a změnit heslo. Pokud to aplikace umožňuje, může účet odhlásit ze všech přihlášených zařízení

O7 - Jaké jsou výhody a nevýhody informování zdroje, že jste ztratili telefon?

- Diskuse bez správných odpovědí

Dobré zprávy! Kamarád Sáry, který s ní byl na párty, našel její telefon ve svém kabátu. Sáře druhý den zavolal a telefon jí vrátil.

O8 - Sára má telefon zpět. Jaké kroky by měla udělat s ohledem na digitální bezpečnost svého zařízení pro případ, že ho opět ztratí?

- Zvážit občasné využití biometrického zabezpečení. Má to své výhody i nevýhody. Nikdo se Sáře nemůže dívat přes rameno při zadávání hesla a nezachytí to ani kamerové systémy, zároveň ji je ale snazší přimět, aby zařízení odemkla
- Použít delší heslo či přístupovou frázi pro přístup do telefonu. Je vhodné se vyhnout odemykání zařízení pomocí vzorů (například spojování teček). Je totiž snadné heslo napodobit, když ho někdo zahlédne, natočí ho kamera nebo ho útočník rozpozná ze šmouh na displeji
- Pokud má Sára obavu, že by se k jejímu telefonu mohl někdy opět dostat někdo jiný, měla by zvážit uzamčení některých aplikací (například těch pro zasílání zpráv) pomocí samostatného hesla
- Nastavit si aplikace umožňující vysledování ztraceného nebo odcizeného zařízení, případně jeho kompletní vymazání

O9 - Jak by z pohledu organizace měl vypadat dobrý nástupní proces pro nové zaměstnance? Jak by měla být zabezpečena jejich zařízení jako telefony a počítače?

- Ujistěte se, že všechen personál bez ohledu na postavení projde vstupním školením a pochopí jeho důležitost
- Organizace by měly jasně specifikovat požadavky na personál stran digitální bezpečnosti
- Identifikovat kroky, které je třeba udělat, pokud dojde ke kompromitaci zařízení (odcizený telefon, prolomené heslo)
- IT podpora by se měla věnovat všem uživatelům, kteří to potřebují

Příběh 2: Provozní bezpečnost

Vytvořeno účastníky programu JSF

Cíl

Zvýšit povědomí účastníků ohledně digitální bezpečnosti a seznámit je s ověřenými postupy, které mohou zavést v rámci jejich organizace, ale též se svými spolupracovníky či novináři na volné noze

Vzdělávací cíle

1. Teoreticky porozumět konceptu digitální bezpečnosti jakožto nikdy nekončícího procesu
2. Mluvit s ostatními, učit je a vysvětlit jim důležitost digitální bezpečnosti
3. Prodiskutovat praktické možnosti bezpečné komunikace pomocí mobilního zařízení (laptop, tablet, mobilní telefon)
4. Poskytnout ověřené postupy bezpečné práce s digitálními soubory
5. Zvýšit povědomí o bezpečném nastavení účtů v rámci propojené počítačové sítě
6. Porozumět důležitosti modelování rizik

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci

1. Nastavení a údržba oprávnění na platformách pro spolupráci (např. Disk Google)
2. Prohlížení přístupových protokolů na platformách pro spolupráci, jako je Disk Google. (Pokud je to možné. Některé z těchto funkcí jsou totiž dostupné pouze na podnikových aplikacích)
3. Nastavení a využívání dvoufázového ověřování, nejlépe zabezpečeného fyzickým bezpečnostním klíčem či podobným mechanismem, který je odolný vůči phishingu
4. Dodržování zásad pro účinná hesla (používání jedinečných a dlouhých hesel či přístupových frází) a využívání správců hesel
5. Šifrování dokumentů (např. Využitím Mailvelope)
6. Instalace, nastavení a využívání aplikace Signal (nebo jiné zabezpečené aplikace pro zasílání zpráv).
    a. A také využívání pokročilých funkcí těchto aplikací, jako je automatické mazání zpráv
7. Instalace, nastavení a využívání služby Mailvelope nebo jiných šifrovaných e-mailů
8. Bezpečná práce se soubory a dokumenty od citlivých zdrojů

Příběh

Sára dává dohromady tým novinářů, aby prošetřili korupci při zadávání veřejných zakázek ministerstvem zdravotnictví během pandemie koronaviru. Ne všichni v týmu mají stejnou úroveň

digitálních dovednosti, znalostí a postupů v oblasti digitální bezpečnosti. Sára ví, že jeden z členů jejího týmu je na tom velmi špatně se zabezpečením souborů.

O1 - Jak může Sára povzbudit své kolegy, aby zlepšili svůj přístup k digitální bezpečnosti? Co by měla udělat, aby zajistila dostatečnou úroveň digitální bezpečnosti ve svém týmu?

- Vysvětlit, proč je důležité kvalitní digitální zabezpečení. Může mluvit o tom, jak může špatná digitální bezpečnost ohrozit kariéru novináře, či o tom, že s větší bezpečností jim pravděpodobně budou i více důvěřovat jejich zdroje a kolegové. Zároveň nejde jen o to, aby chránili sebe, ale také ostatní kolem nich.
- Prodiskutovat následující:
    a. jaká zařízení kdo používá
    b. jak mají zabezpečené své uživatelské účty
    c. jak skladují a předávají digitální soubory
    d. pomocí jakého zařízení se přihlašují do pracovní sítě (využívají vlastní zařízení, nebo pracovní?)
    e. využívají dvoufázové ověření pro vyšší bezpečnost svých účtů
    f. jak přistupují ke svým heslům (mění svá hesla, využívají správce hesel)
- Rozhodněte, jak by tým měl komunikovat, uchovávat a sdílet soubory. Smyslem druhého kroku je, aby všichni dodržovali ty samé postupy
- Zvažte trénink týmu s ohledem na nově nastavené postupy. Po stanovení nových pravidel by tým měl “nanečisto” otestovat nové metody komunikace a případně odladit nedostatky

O2 - Jak by Sára a její tým měl uchovávat a sdílet audio soubory a dokumenty od zdrojů?

- Omezit přístup k různým souborům a složkám a s opatrností využívat možnosti sdílení v aplikacích, jako je Disk Google
- Uvědomit si bezpečnostní principy v situacích, kdy vynáší soubory či dokumenty mimo pracovní prostředí (USB klíče, přílohy e-mailu,...). Tyto situace mohou rozšířit možnosti pro útoky a zvýšit riziko úniku informací
- Požádat tým, aby k přístupu k pracovním souborům vždy používal výhradně pracovní počítače
- Omezit možnosti toho, co lze na pracovní počítače instalovat, a zajistit, aby na těchto zařízeních byla vždy silná hesla a aktuální software

O3 - Jak Sára a její tým zajistí bezpečnou komunikaci?

Sára může zajistit bezpečnou komunikaci týmu tím, že všechny naučí používat stejnou komunikační platformu, která se bude kolegyním a kolegům pohodlně používat.

Zvažte:

- Přesun většinu konverzací do aplikace Signa, mizející zprávy a kopírování zpráv, které je nutné zachovat

- Neodesílat citlivé informace mimo doménu organizace, jelikož nebude fungovat šifrování
- Využívání protokolu PGP v e-mailu
- Vytvoření přísných pravidel pro zabezpečení e-mailových účtů (jedinečná hesla, dvoufázové ověření)

Dva týdny před zveřejněním zprávy Sáře zavolá hlavní vládní zdroj této investigace. Sára ho dobře zná a důvěřuje mu. Během hovoru zdroj jednoduše řekne: „Vláda to ví - došlo k úniku informací“ a zavěsí.

O4 - Co jsou z pohledu digitální bezpečnosti první kroky, které by Sára měla udělat tváří v tvář možnému úniku informací?

- Požádat všechny členy jejího týmu, aby si změnili hesla pro případ, že by útočník získal přístup k některému z jejich účtů.
- Zvážit skutečnost, že vláda nemusela nutně proniknout do její redakce; je možné, že se o úniku dozvěděla třeba tak, že zjistila, kteří vládní zaměstnanci co tiskli
- Provést průzkum uvnitř redakce: ověřit, zda všichni dodržovali protokoly, zjistit jaké informace či soubory přesně unikly a kdo k nim měl přístup. Využitím kontroly přístupu a verzí si může usnadnit sledování přístupu k jednotlivým částem dat, na kterých pracuje
- Je vhodné se zamyslet, jestli není potřeba uspíšit publikaci zjištění

Sára zjistila, že k úniku došlo z její redakce. Jeden z designérů měl přístup ke sdílenému Google Disku organizace.

Sára se o tom dozvěděla tak, že zkontrolovala záznam o přístup k Google Disku a zjistila, že tým designérů má, vzhledem k povaze své práce, přístup ke všemu ve společné síti. Všimla si, že jeden z nich omylem sdílel dokument s externím klientem. Ten pracoval pro vládu a měl shodou okolností stejné příjmení, jako kolega v práci.

O5 - Co v téhle Situaci měla Sára dělat jinak?

- Sára by měla zavést bezpečné postupy, které chrání její investigativní tým. Měla by zajistit, aby existoval postup pro schvalování a řízení přístupů, který bude dodržován.
- Tým by měl s designéry pracovat tak, aby měli k dispozici jen informace, které skutečně potřebují. Neměly by jim být poskytovány žádné tajné nebo citlivé údaje, pokud to není pro publikaci nezbytně nutné
- Sára by také měla považovat bezpečnost a soukromí za proces, nikoli za stav. Je to totiž něco, co by se mělo neustále zdokonalovat

Příběh 3: Obtěžování a doxxing

Vytvořeno účastníky programu JSF

Cíl

Pomoci účastníkům vytvořit si představu o tom, jak se nejlépe připravit na doxxing a obtěžování v digitálním prostoru a jak na to reagovat

Vzdělávací cíle

1. Identifikovat obranné metody a opatření pro novináře, kteří se potýkají s obtěžováním na sociálních sítích a doxxingem
2. Pochopit, jak mohou být informace zveřejněné na sociálních médiích snadno přístupné a zneužitelné proti novinářům
3. Zjistit, jaký je vztah mezi genderem, obtěžováním a jeho důsledky pro bezpečnost
4. Prodiskutovat, jaké postupy a praktiky může zavést mediální organizace, aby ochránila své zaměstnance a partnery, kteří jsou terčem doxxingu a obtěžování
5. Prodiskutovat pohotovostní plán pro novináře, kteří nemají zázemí a podporu redakce (např. novináři na volné noze, externí zaměstnanci)
6. Šířit osvětu o bezpečnosti a naučit se přesvědčivě vysvětlit, že obtěžování je závažný problém, který vyžaduje koordinované kroky a podporu uvnitř organizace, a to i lidem, kteří se s ním běžně nesetkávají
7. Zabezpečení organizací: nastavení postupů a procesů v rámci organizací, vymýšlení způsobů, jak mohou organizace co nejlépe podpořit novináře, kteří čelí obtěžování

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci

1. Správa a aktualizace nastavení ochrany osobních údajů na předních sociálních sítích
2. Používání bezpečnostních nástrojů, jako je nahlašování a blokování, na těchto platformách. A to včetně pochopení jejich mechanismů a využití
3. Nastavení a používání dvoufaktorového ověřování, ideálně pomocí fyzických bezpečnostních klíčů nebo podobných mechanismů odolných proti phishingu

Příběh

Sára pracuje na článku o etnických menšinách v její zemi a o tom, jak vládní politika vede k jejich větší marginalizaci. V průběhu posledních týdnů Sára zaznamenala nárůst komentářů na jejích účtech na sociálních médiích, kde běžně sdílí své pracovní výstupy. Zaměřili se na ní i online trolové, kteří ji pod příspěvky píší nenávistné a urážlivé komentáře.

O1 - Jaké kroky může Sára podniknout, aby zablokovala a nahlásila autory těchto komentářů?

- Může využít blokovací a nahlašovací funkce, které jsou zabudované ve většině sociálních médiích
- Může sama nebo pomocí své organizace kontaktovat provozovatele sociálních médií a nahlásit dlouhodobé a rozsáhlejší obtěžování
- Zakázat zveřejňování příspěvků a komentářů na jejím profilu
- Omezit možnosti, kdo ji může na sociálních sítích najít
- Zakázat označování na sítích

Snaha o nahlášení hlavních iniciátorů obtěžování naštvala skupinu trolů, kteří začali vytvářet a šířit další nenávistný obsah namířený proti Sáře. Některé z komentářů rovněž obsahují přímé a nepřímé výhrůžky násilím.

O2 - Jakými cestami může Sára zjistit, zda je nenávisti vůči ní součástí větší koordinované kampaně, či jde o organický obsah?

- Může věc zkoumat sama, případně poprosit kolegyně a kolegy o pomoc
- Může prověřit, zda všichni trollové používají stejný jazyk, klíčová slova či hashtagy. Pokud ano, pravděpodobně se jedná o koordinovanou kampaň
- áleží na platformě. Například na Instagramu existují rozsáhlé možnosti, jak zobrazit informace o konkrétních účtech - kdy byl vytvořen, kolik lidí ho používá, jak často měnil jméno atd
- Zkontrolovat, jestli se na obtěžování podílí nějaká média
- Podívat se na nejčastější čas, kdy se příspěvky objevují

Řekne kolegům o nenávistných příspěvcích, ale většina jsou muži, kteří jí doporučí se nestresovat. Problém prý po čase sám zmizí. Sára je vystresovaná, má pocit, že jí tým nenaslouchá nebo nerozumí problému.

O3 - Místo uklidňování Sáry, že se nemá ničeho obávat, jakým způsobem ji může její tým a organizace podpořit, zejména ve vztahu k přítomnosti online a digitální bezpečnosti?

- Pomoci situaci prověřit
- Projít se Sárou její digitální bezpečnostní opatření a pomoci jí některá zlepšit, pokud je to třeba
- Získat doporučení a zkušenosti od ostatních organizací
- Předat přístup k jejímu účtu někomu důvěryhodnému, kdo by se o něj mohl starat, aby Sára nebyla přímo vystavena závadnému obsahu, ale stále měla k účtu přístup
- Organizace obtěžování analyzovat a zjistit, zda v něm nenajde opakující se vzorce
- Zmapovat, jak obtěžování probíhá, a to skrz příspěvky organizace, nikoli Sáry
- Přesunout pátrání na bezpečnostní tým, které s ním může pomoci

Jednoho dne zveřejní trollové Sářiny fotky. Jde o několik let staré fotografie ze sociálních sítí, jsou soukromé a některé obsahují citlivé informace.

Vstup - Dejte účastníkům 1 až 4 fotografie (Fotografie jsou v příloze tohoto scénáře). Příklady fotografií obsahují:

- Sáru, jak venčí psa před svým domem
- Sáru, jak kouří cigaretu s marihuanou
- Sáru s blízkými přáteli na dovolené
- Sáru, jak pracuje v newsroomu

Rozeberte s účastnicemi a účastníky, proč mohou být všechny zmíněné fotografie citlivé.

O4 - Jakými cestami se někdo mohl dostat k online informacím o Sáře, např. starým příspěvkům na sociálních médiích?

- Přátele od Sáry zveřejnili fotografie s nedostatečným nastavením soukromí
- Někdo se naboural do Sářiných účtů
- Je možné, že jeden z jejích kontaktů na sociálních sítí fotografie uložil, aby je později mohl sdílet
- Sářiny fotky na sociálních sítích mohly projít indexováním vyhledávačů

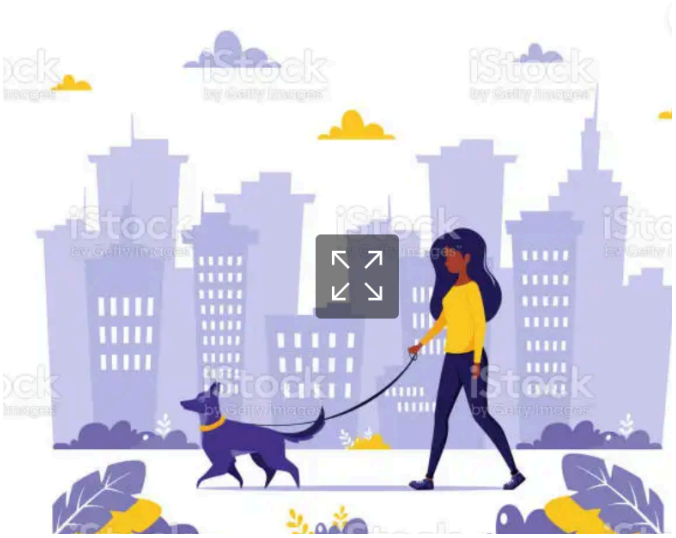
O5 - Jaké kroky může Sára vyzkoušet, aby předešla budoucím únikům osobních informací online?

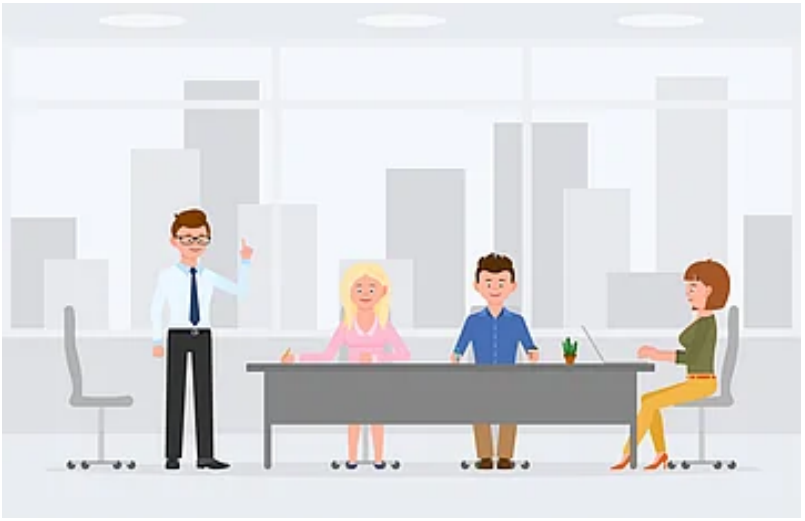
- Smazat staré fotografie
- Smazat účty
- Uzamknout účty
- Nahrát nové fotografie, které o ní ale prozrazují jen málo
- Získat výpis všech informací, které o ní sociální média shromažďují
- Nahlásit fotografie, které byly v poslední době zveřejněny či nahlásit účty, které je zveřejňují
- Pokračovat ve zveřejňování pracovního obsahu, zatímco omezí zveřejňování osobních informací. Pokud svou aktivitu omezí úplně, trollové budou mít vyhráno
- Dokumentovat škodlivé příspěvky pomocí screenshotů a mapovat jména/přezdívky trollů

O6 - Jaké kroky může z hlediska digitální bezpečnosti Sára a její organizace podniknout, aby nedocházelo ke sběru a zveřejňování citlivých informací?

- Omezit viditelnost osobních fotografií a příspěvků jen na skupinu vybraných přátel
- Nezveřejňovat citlivé informace (jako třeba fotku při kouření marihuany)
- Nezveřejňovat fotografie, které ukazují soukromé informace, jako může být místo pořízení
- Může si také otevřít firemní účet, kde by měla pracovní příspěvky, které nesouvisí s jejím osobním životem
- Dodržovat na sociálních sítích bezpečnostní zásady, jako mít nastavené silné heslo a dvoufaktorové ověření

Příloha 1: Příklady fotografií pro vstup





Příběh 4: Bezpečnostní složky se dostaly do redakce

Vytvořeno účastníky programu JSF

Cíl

Dát účastníkům praktické i teoretické postupy jak reagovat na bezpečnostní složky v redakci.

Vzdělávací cíle

1. Zajistit záložní komunikační plány a technické nástroje pro případ, že ztratí přístup do redakce nebo k osobním zařízením
2. Porozumět osvědčeným postupům zabezpečení digitálních zařízení v redakci nebo organizaci
3. Najít způsoby jak zabezpečit různé soubory na digitálním zařízení, například počítači nebo mobilu
4. Mít plán pro případ že bezpečnostní složky provedou v redakci razii zmocní se informací
5. Prozkoumat koncepty modelování rizik a plánování pro jednotlivce i organizace

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci

1. Využívání nástrojů, jako je VeraCrypt, které umožňují šifrování dat na pevných a externích discích
2. Modelování hrozeb zaměřené konkrétně na práci s úřady a razie v organizacích: jak vyhodnotit rizika, připravit se na ně a provést následné zhodnocení
3. Bezpečnost v organizaci a komunitách: konkrétně jak pracovat s redaktory, manažery a právníky ve vypjatých situacích a jak určit, který problém předat kterému člověku
4. Práce s nastavením uvnitř aplikací Microsoft Office a Google Drive se záměrem zjistit, kdy a do jakých souborů bylo v poslední době nahlíženo
5. (Pro pokročilé) Přístup k protokolům o přístupu a práce s nimi protokoly prostřednictvím prémiového předplatného Google Drive nebo O365, pokud k nim má organizace přístup
6. Procházení historie vyhledávání a přístupů k souborům v předních webových prohlížečích a operačních systémech

Příběh

Sára pracuje týmu asi 20 lidí. Je rušné pondělní ráno, 15 novinářů pracuje v redakci a dalších 5 z domova.
V 10 hodin do redakce přijde asi 50 policistů. Mají povolení k prohlídce, které ukážou editorovi a pak se protlačí do redakce, zatímco požadují aby všichni zaměstnanci okamžitě odešli.

Sára a její kolegové a kolegyně čekají venku a probírají, jak udržet reakci v chodu a jak ji zabezpečit.

O1 - Jaké jsou priority v podobných situacích?

- Spojit se s právníkem a prodiskutovat s ním další kroky
- Kontaktovat kolegy, kteří pracují na dálku
- Zjistit, kdo má u sebe mobilní telefon a kdo ho nechal v redakci

O2 - Jak může Sára a její tým v této situaci komunikovat bezpečně?

- Vytvořit skupinu na WhatsAppu či Signalu
- Je dobré zvážit, zda nekomunikovat spíše přes soukromá čísla než pracovní. Konverzace totiž mohou být synchronizovány se zařízeními, která stále jsou v redakci

O3 - Jak mohou zabezpečit redakční online účty, např. webové stránky nebo sociální sítě?

- Okamžitě změnit hesla
- Odhlásit se na dálku ze zařízení, která jsou v redakci, pokud je to možné. Toto rozhodnutí je ale důležité nejdříve konzultovat s právníky, aby nebylo považováno za nezákonnou manipulaci s důkazy (to se liší podle zákonů dané země)
- Probrat s právníky možnosti zveřejnění informací o policejní razii

Sára si pamatuje že při odchodu z redakce viděla, jak policisté berou nějaké dokumenty, počítače a jiná zařízení. Svůj telefon si zvládla odnést, ale laptop v redakci zůstal. Tým se snaží zjistit, jaké informace se policii podařilo získat.

O4 - Jak by měly být zabezpečeny redakční zařízení?

- Počítače chráněné silnými hesly
- Nastavit krátké intervaly pro zamykání obrazovky?
- Šifrované USB disky a externí harddisky

Z diskuze vyplyne, že se editorovi při odchodu z kanceláře nepodařilo zamknout svůj počítač.

O dvě hodiny později policie opustí redakci a novináři mohou zpět. Zaměstnanci se sejdou a diskutují jaké informace policie mohla získat a zda podobné riziko hrozí i v budoucnu.

O5 - Jak může redakce okamžitě vyhodnotit dopad zásahu?

- Ověřit, jaké dokumenty byly odneseny nebo přerovnány (pokud byly složky na jiném místě než předtím, je možné, že si je policisté vyfotili)
- Na počítačích je obvykle možné zkontrolovat historii vyhledávání/přístupu k souborům/prohlížeče. V aplikaci Microsoft Word si lze prohlédnout i poslední otevřené soubory. A v případě, že používáte Dokumenty Google, i historii úprav.

Pokud byla historie souborů vymazána, znamená to také, že se někdo mohl pokusit zamést za sebou stopy
- Je nepravděpodobné, že by byl během zásahu nainstalován nějaký malware, ale pokud se toho obáváte, poraďte se s odborníkem specializujícím se na forenzní analýzu malwaru

O6 - Jak může organizace zajistit, že je razie nemůže dále ohrožovat?
- Změnit pro jistotu hesla
- Poraďte se s právníkem o tom, k čemu policie měla a neměla povolení mít během zásahu přístup
- Pokud pro svou práci pracovníci organizace používali krycí jména či pseudonymy, je na místě je změnit

O pár týdnů později svolá editor redakci dohromady. Chtějí zjistit jakým podobným rizikům by mohli čelit.

O7 - Z pohledu modelování rizik a digitální bezpečnosti: kde novináři i redakce vidí hrozící rizika?
- Položte si základní otázky pro modelování hrozeb: Jaké informace máme k dispozici? Kdo by mohl mít zájem se k nim dostat? A co by se stalo, kdyby se mu/jim to podařilo?
- Vytvořte si seznam možných narušitelů a přemýšlejte o jejich motivech (co by chtěli udělat a proč) a schopnostech (co jsou skutečně schopni udělat, jaké mají technické, právní, organizační a finanční prostředky).

Příběh 5: Bezpečnostní složky se dostaly k novináři domů

Vytvořeno účastníky programu JSF

Cíl

Dát novinářům teoretické a technické dovednosti a pomoci jim nastavit doma co nejbezpečnější prostředí.

Vzdělávací cíle

1. Naučit se, jak zabezpečit domácí digitální zařízení
2. Nastavit bezpečnostní opatření kolem papírových zápisků
3. Představit vzdálené mazání souborů a výhody i nevýhody které to obnáší
4. Omezení přístupu k informacím, které byly kompromitovány
5. Připravit se na vstup bezpečnostních složek do novinářova domu
6. Nasměrovat účastníky, aby se zamysleli nad zabezpečením organizací a komunit. Konkrétně by měli zvážit, jak pracovat s redaktory, manažery a právníky ve vypjatých situacích a jak určit, který problém předat kterému člověku

Dovednosti a přístupy chování, které je potřeba procvičit před nebo po simulaci

1. Využívání nástrojů, jako je VeraCrypt, které umožňují šifrování dat na pevných a externích discích
2. Modelování hrozeb zaměřené konkrétně na práci s úřady a razie v organizacích: jak vyhodnotit rizika, připravit se na ně a provést následné zhodnocení
3. Aktivace nástrojů, jako je Apple Find My nebo Android/Samsung Find, které lze použít ke vzdálenému uzamčení nebo vymazání zařízení
4. Práce s nastavením uvnitř aplikací Microsoft Office a Google Drive se záměrem zjistit, kdy a do jakých souborů bylo v poslední době nahlíženo
5. (Pro pokročilé) Přístup k protokolům o přístupu a práce s nimi protokoly prostřednictvím prémiového předplatného Google Drive nebo O365, pokud k nim má organizace přístup
6. Procházení historie vyhledávání a přístupů k souborům v předních webových prohlížečích a operačních systémech

Scénář

5 měsíců po parlamentních volbách začala nová vláda omezovat svobodu tisku. Bezpečnostní složky provedly razii v domě tří prominentních novinářů v hlavním městě. V reakci na to se Sára sešla s pár kolegy a probírali, jak se bránit a zabezpečit jejich informace, pokud by se jim stalo něco podobného.

O1 - Co by měli novináři zvážit pokud se rozhodnou uchovávat informace doma

- Uchovávat zařízení na bezpečném místě
- Hesla a šifrování na všech zařízeních
- Neuchovávat informace o citlivých zdrojích, jako například jejich jména na dokumentech
- Udržovat inventář kde jsou uchovány jaké informace (ale i ten zabezpečit!)
- Analogové informace: myslete na fyzické kopie
- Pokud je možné uchovávat citlivé informace jinak než doma, je dobré to zvážit
- Sledovat místní zákony a bezpečnostní pravidla organizace
- Být si vědomi důsledků skladování citlivých informací doma namísto vaší kanceláře
- Zamyslet se nad tím, kdo má přístup do vašeho domova a k vašim zařízením

O2 (volitelná) - Jaké jsou osvědčené postupy pro uchovávání papírových zápisků doma?

- Zvažte zničení toho, co už nepotřebujete
- Nenechávejte všechny poznámky na jednom místě
- Schovejte zápisníky
- Trezor, zámek a klíč - zabezpečte je!
- Jak moc citlivé informace mají být uchovávány doma?
- Používat zkratky, krycí jména, těsnopis - něco co pochopíte jen vy

O3 - Jaká opatření mohou co nejvíce zabezpečit elektronická zařízení (počítače, harddisky, USB disky atd)

- Šifrování
- Ochrana hesel
- Zálohování dat na jiném místě
- Promyslete zabezpečení starších zařízení, zejména těch, která už nepoužíváte

Dnes Sára odešla z domova v 9, nakoupit potraviny a kávu. Když se vrátila o hodinu později, dveře jejího bytu byly otevřené. Sára vešla dovnitř a našla dva muže jak prohledávají její stůl a ložnici. Jeden z nich si pročítá Sářiny zápisníky a druhý drží tašku s jejím laptopem. Sára vidí, že ze stolu zmizely USB disky a externí harddisky. Muži jsou v civilu, ale Sára předpokládá, že pracují pro vládu.

Možnost 1 - Sára s oba muži krátce promluví a může bezpečně opustit domov. Jde ke kamarádce, která bydlí nedaleko.

O4 (volitelná) - Pokud Sára ví, že některé informace, zejména papírové zápisníky, byly kompromitovány, koho má o incidentu informovat?

- Informujte o tom editora a právní oddělení redakce
- Než se spojí se zdroji, které mohly být v zápisníku zmíněny, měla by si o tom nejdříve promluvit uvnitř redakce (s vedením redakce, kolegy, bezpečnostním oddělením). Pokud by byly zdroje v dokumentech zmíněny pod pseudonymem,

jejich kontaktování by mohlo vést k identifikaci. Je proto někdy moudřejší vyčkat a zdroje nejdříve neoslovovat.

O5 - Co může Sára udělat, aby zabránila dalšímu přístupu k jejím digitálním informacím dokud jsou muži stále v jejím bytě?

- Udělat vše co může abyste dodrželi místní zákony
- Trvat na tom, aby i bezpečnostní složky dodržely zákony (např. Dovolit natáčení, svědky atd)
- Techniky deeskalace
- Zjistit kdo jsou a jaký mají mandát/povolení k prohlídce
- Zhodnotit situaci z hlediska její vlastní bezpečnosti
- Vyhledat právní pomoc, zavolat do redakce
- Předložit falešné doklady a dokumenty (může vyžadovat přípravu)
- Odklonění pozornosti

Možnost 2 - Sára nemůže opustit svůj byt. Dva muži po ní chtějí hesla k počítací a USB diskům. Vyhrožují jí, že ji vezmou na policejní stanici pokud informace neposkytne. Sára se ptá na příkaz k domovní prohlídce, ale žádný nemají.

O6 - Pokud Sára ví, že má na počítači citlivé informace, včetně těch, které mohou odhalit tajné zdroje, co může v této situaci udělat?

- Zhodnotit zranitelnost a prioritizovat nejdůležitější věci
- Přihlásit se na dálku a smazat citlivé účty
- Identifikovat všechny informace které měla doma
- Zvážit klady a zápory informování ostatních členů týmu a zdrojů, které mohou být ohroženy. Případně toto rozhodnutí udělat s podporou redakce
- Potenciál vzdáleného mazání souborů

O7 - Sára má na počítači program pro vzdálené mazání souborů. Co musí promyslet než soubory smaže?

- Může to být trestný čin - maření spravedlnosti
- Měla by se nejdříve poradit s právníkem o možných důsledcích tohoto kroku
- Jestliže Sára nemá důkazy o tom, že jde o osoby z orgánů činných v trestním řízení, ale vypadají jako standardní narušitelé nebo z nestátní bezpečnostní složky, mění se tím i právní situace a hrozby

O8 (volitelná) - Koho má Sára informovat o incidentu, s vědomím, že její informace byly kompromitovány? Je pořadí lidí, které informuje, důležité?

- Editor
- Bezpečnostní/IT team
- Právní oddělení redakce
- Zvážit informování zdrojů

- Pokud pracuje na volné noze, zvážit že dá vědět ostatním novinářům na volné noze.

Sára nakonec odmítne sdělit svá hesla. Potom, co muži dalších 10 minut prohledávají její domov, odejdou s jejím laptopem, USB disky a papírovým zápisníkem.

Sára má zase přístup do svého bytu. Vidí, že jeden z jejích dvou počítačů tam zůstal spolu s jedním USB diskem. Všechny papírové zápisníky odnesli.

O9 - Co by měla Sára nyní udělat, aby se ujistila, že její informační bezpečnost není ohrožená tím co muži udělali, zatím co byli u ní doma?

- Mohli do nějakého zařízení nainstalovat škodlivý software; možná by bylo dobré poslat tato zařízení specialistovi na digitální forenzní analýzu
- Uvědomit si, že její byt mohl být napíchnutý
- Zjistit možnosti podpory uvnitř své organizace
- Promluvit si s právními a bezpečnostními poradci o tom, zda má z hlediska bezpečnosti a zabezpečení větší smysl o razii veřejně mluvit, nebo ne

O10 (volitelná) - Kromě digitálních aspektů scénáře, jaká další opatření mohla Sára provést, aby zajistila bezpečnost svou i svých informací?

- Zjistit více informací o fungování bezpečnostních složek v zemi. Ověřit si, zda mohou existovat skupiny, které se snaží zastrašovat novináře, ale nejsou spojeny s bezpečnostními složkami
- Připravit se s právníky a redaktory na to, jak příště lépe reagovat na domovní prohlídky
- Pokud jsou domovní prohlídky reálnou hrozbou, je lepší neskladovat citlivé informace doma